Title: Jalangi: A Dynamic Analysis and Concolic Testing Framework for JavaScript

Speaker: Dr. Koushik Sen  
Associate Professor  
University of California Berkeley

Date/Time: 22 July 2014, Tuesday, 11:00 AM to 12:00 PM

Venue: MR1, COM1-03-19

Chaired by: Dr Roychoudhury, Abhik, Professor, School of Computing  
(abhik@comp.nus.edu.sg)

Abstract:

JavaScript is the most popular programming language for client-side web programming. Advances in browser technologies and JavaScript engines in the recent years have fueled the use of JavaScript in Rich Internet Applications, and several mobile platforms including Android, IOS, Tizen OS, Windows 8, Blackberry, and Firefox OS, support applications written in JavaScript/HTML5. With a renewed interest in JavaScript, many complex applications such as Google docs, Gmail, and a variety of games are being developed using HTML5/JavaScript. However, unlike C/C++, Java, and C#, JavaScript is significantly shorthanded in the tools landscape. The dynamic and reflective nature of JavaScript makes it hard to analyze it statically.

I will talk about the Jalangi project which investigates a dynamic analysis framework and several dynamic analysis techniques for JavaScript. The analysis framework provides a few useful abstractions and an API that significantly simplifies implementation of dynamic analyses for JavaScript. The framework works through source code instrumentation and allows implementation of various heavy-weight dynamic analyses and test generation techniques. The projects investigates and implements several dynamic analyses including concolic testing, pure symbolic execution, a detector of likely type inconsistencies, and a runtime memory profiler. The techniques developed in this project are suitable for analyzing and testing that web applications written in JavaScript/HTML5 are free of common correctness and performance bugs.

Biography

Koushik Sen is an associate professor in the Department of Electrical Engineering and Computer Sciences at the University of California, Berkeley. His research interest lies in Software Engineering, Programming Languages, and Formal methods. He is interested in
developing software tools and methodologies that improve programmer productivity and software quality. He is best known for his work on ?DART: Directed Automated Random Testing? and concolic testing. He has received a NSF CAREER Award in 2008, a Haifa Verification Conference (HVC) Award in 2009, a IFIP TC2 Manfred Paul Award for Excellence in Software: Theory and Practice in 2010, a Sloan Foundation Fellowship in 2011, and second Professor R. Narasimhan Lecture Award in 2014. He has won three ACM SIGSOFT Distinguished Paper Awards. He received the C.L. and Jane W-S. Liu Award in 2004, the C. W. Gear Outstanding Graduate Award in 2005, and the David J. Kuck Outstanding Ph.D. Thesis Award in 2007 from the UIUC Department of Computer Science. He holds a B.Tech from Indian Institute of Technology, Kanpur, and M.S. and Ph.D. in CS from University of Illinois at Urbana-Champaign.